# Secure Transfer of Several Images Using the Same Frame

IVANA RAKO¨EVI˘ [1], BRANIMIR RELJIN [2], PAVLE KOSTI˘ [2], IRINI RELJIN [3]
and NIKOS MASTORAKIS[4]
[1] TMS Project, [2] Faculty of Electrical Engineering, [3] PTT College

YUGOSLAVIA
[4]Military Institutions of University Education, Hellenic Naval Academy,
Terma Hatzikyriakou, 18539, Piraeus, GREECE

*Abstract*: The possibility of the secure transfer of several digital images using the same frame is described. Our approach is based on the fact that the main part of the signal energy is concentrated in the low-frequency (LF) part of the spectral domain, producing these spectral components have the main influence on the image intelligibility. By using this fact it is possible to reconstruct the image, retaining satisfactory image quality, by using only the LF part of the image spectra and filling the rest of the spectral matrix by zeros. Consequently, in the spectral matrix the existence of the empty part appears. In this empty part the spectral components of another images, we want to be encrypted, could be placed. The image retaining the original LF position in the spectral matrix will be visible during the transfer and we call it the *background image*. Another image (or images) whose spectral components are replaced inside the empty parts of the transform matrix is invisible i.e. it is the *encrypted image*, till the reconstruction process. By appropriate replacement the LF parts of several images into the transform matrix we can obtain secure transfer of these images without significant mutual influence. The procedure described is performed in the FFT domain, for the full-sized images, as well as in the DCT domain, for the 8x8 pixels blocks, having in mind the JPEG image compression.

*Key-Words:* FFT, DCT, image encryption, image intelligibility, JPEG compression
CSCC99 Proceedings: pp.7241-7245

## 1 Introduction

Everyday use of modern communications requires data protection against unauthorized access. This problem is significant particularly in video and digital image transfer via computer network. One possible protection technique is digital watermarking [1],[2] which embedded the watermark signal inside the image content in order to define the owners property of the digital product.

Here we exposed one possible method for a protected transfer of digital images. This method is based on the fact that satisfactory quality of reconstructed image can be achived by using its low-frequency (LF) part in the transform domain.

One possible protected transfer of digital images, using the Fourier transform domain, is presented in Section 2. In Section 3 the digital image reconstruction method, using the LF parts of the amplitude and the phase Fourier transform matrices, is given. We also described the influence of the preserved spectral components to the reconstruction quality. It is shown that by using only … of amplitude and … of phase spectra in the LF domain, a satisfactory good reconstruction quality is achived. That rises the possibility for protected transfer, described in Sections 4 (using Fourier transform – FFT) and 5 (using discrete cosine transform – DCT). In the empty part of the transform matrix we can place the spectral components of another image which needs protection. Image retaining the original spectral position of LF components is visible during the transfer and we call it the *background image*. Another image whose spectral component is replaced inside the empty transform matrix parts is invisible i.e. *encrypted image*.

## 2 The Significance of the Phase on the Image Intelligibility

Phase spectral components have the main influence on the image intelligibility [3]. Very impressive example for this is published in [3],[4] where it is shown that, in the FFT domain, using the phase spectrum of one image, say $x(n_1,n_2)$, and the magnitude spectrum of another image, $y(n_1,n_2)$, the image $x(n_1,n_2)$ will be recognized. We can use this phase feature for image encryption. Using the phase matrix of an image we can encrypt the image contents [5]. One possibility of the protected transfer method based on this feature is shown in Figure 1. The results of the applied method are shown in Figure 2.

For instance, let us observe the original image as in Figure 2a, while the background image is in Figure 2b. On the transmitting side the amplitude and phase spectral components of the original image which need to be encrypted are determined. On this side the phase spectral component of the background image which is used to hide the contents of the original image is also determined. Then we multiply, in the spectral domain, the amplitude transform matrix of the original image and the phase transform matrix of the background image. After applying the inverse Fourier transform (IFFT) we obtain the image containing mainly the contents of the background image, as shown in Figure 2c. That image and the phase matrix of the original image are transmitted through the same communication channel.

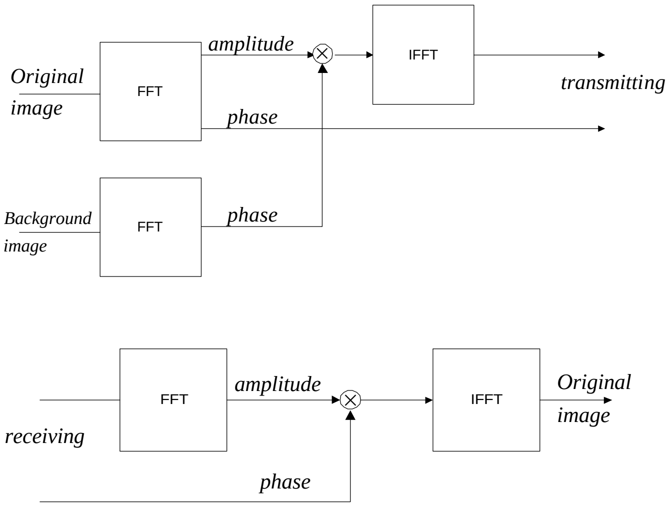



**Figure 1.** Encryption of the Original image contents by using the phase spectrum of the Background image

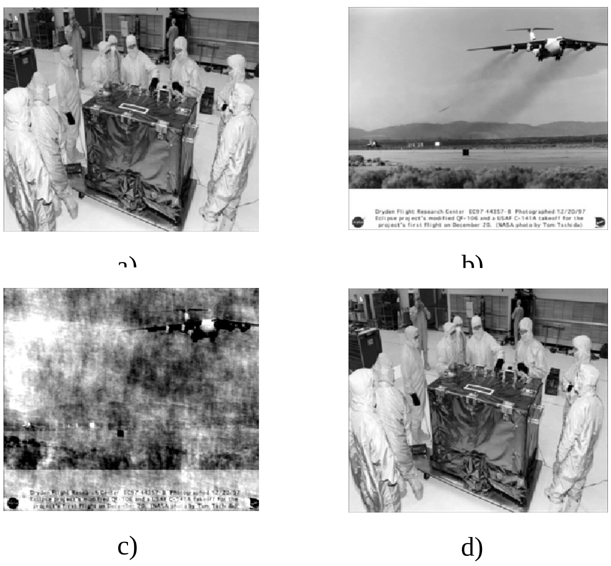



**Figure 2.** Results of the method exposed in Figure 1.

On the receiving side we compute the amplitude spectral components of the received image and we multiply it with the phase transform matrix of an original image, which was also received. After applying Inverse Fourier Transform (IFFT) we obtain very good reconstruction of the original image, as in Figure 2d.

## 3 Digital Image Transfer Using the Parts of Spectral Matrices

Here, we considered the reconstructed image quality obtained by preserving only the LF parts of amplitude and phase Fourier transform matrices. It is known that the LF spectral domain contains the main part of the signal energy. Consequently, this spectral domain keeps the information of image contrast and luminosity.

Here we computed the influence of the preserved spectral component on the reconstructed image quality. All images used in these examples have the resolution of 256 x 256 pixels.

Let us observe again the image in Fig. 2a. First, we used only the … of amplitude- and phase spectral matrices of the image, in the LF domain, as shown in Figs. 3a and 3b, respectively. The other coefficients in these matrices are replaced by zero. After applying IFFT, the reconstructed image is as in Figure 3c, while the absolute error between the reconstructed (Fig. 3c) and the original (Fig. 2a) images is depicted in Fig. 3d.

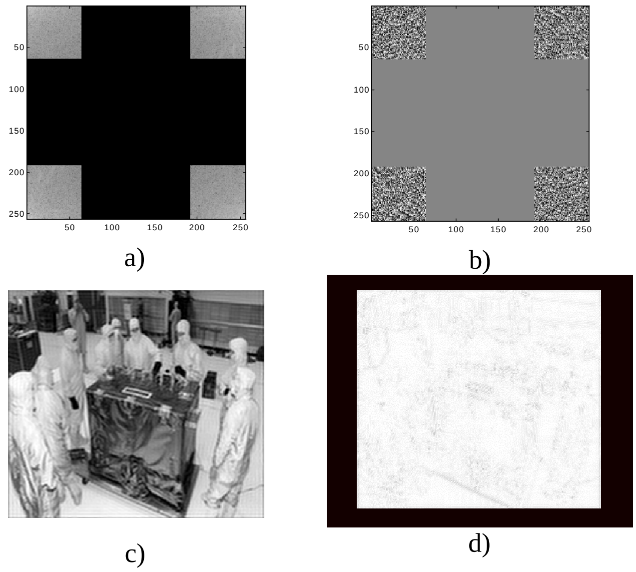



**Figure 3.** Image reconstruction based on the use of … of the amplitude and phase spectral matrices of the image in Fig. 2a.

The same reconstruction method is applied to another pair of spectral matrices but using ¾of spectral coefficients from the LF domain in the amplitude and phase spectra, Figs. 4a and 4b. The reconstructed image and appropriate absolute error are depicted in Figs. 4c and 4d, respectively.

As an objective measure of the error between the reconstructed images $x_R(n_1,n_2)$ in Figs. 3c and 4c and the original image $x(n_1,n_2)$ in Fig. 2b, we can use the normalized mean-square error $x_R$ defined by

$$x_R = \frac{1}{N^2}\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\left(x(n_1,n_2) - x_R(n_1,n_2)\right)^2 \qquad (1)$$

where $N^2$ is an image size (here $n_1 = n_2 = N = 256$).

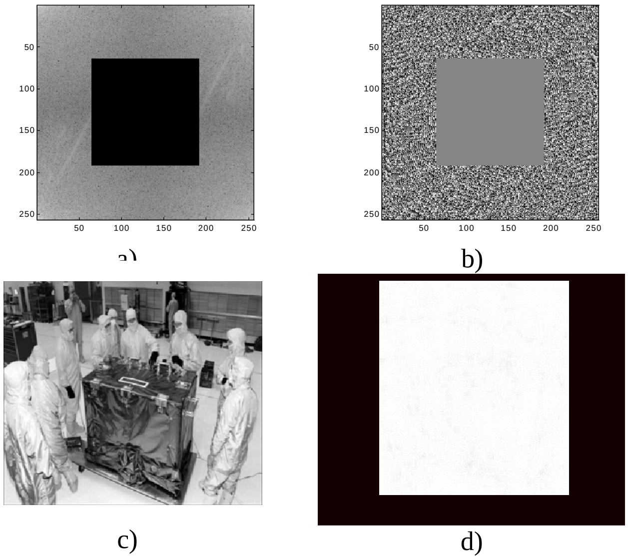



**Figure 4.** Image reconstruction based on the use of ¾of the amplitude and phase spectral matrices of the image in Fig. 2a.

The values of normalized mean-square errors for the images reconstructed by using … and ¾of LF spectral coefficients are presented in Table 1. A good visual quality of digital image reconstruction by using ¾of LF spectral coefficients is confirmed by a low value of the normalized mean-square error presented in Table 1.

**Table 1.** Normalized mean-square errors for reconstructed images in Figs. 3c and 4c

| Amount of LF spectral coefficients | … | ¾ |
|---|---|---|
| Normalized mean-square error $x_R$ | 114.2222 | 6.4476 |

## 4 Digital Image Encryption in the Transform Domain

Using the procedure described in the previous section, the significant part of spectral matrices (Figs. 3a-b) is filled by zeros. We can use these empty parts for the spectral content of another image [6].

Let us observe images as in Fig. 5. We can use … of spectral coefficients of the first image (Fig. 5a), in the LF domain, and ¾ of spectral coefficients of another image (Fig. 5b). Then we can mix their spectral coefficients in the following way. For the first image we retain original positions of spectral coefficients. In the empty parts of the magnitude and phase matrices of this image we can embed the spectral contents of another image, but in reverse order. That means we put the natural LF parts of this image in the HF part of spectral matrices, using `fftshift` Matlab command, as depicted in Figs. 6a and 6b, for, respectively. In this way, after applying IFFT, the image with natural spectral positions (Fig. 5a) will be visible (as a background image), as depicted in Fig. 6c. The hidden image (in Fig. 5b) is invisible till the reconstruction process. The reconstructed encrypted image, by using ¾ of its spectral coefficients, is depicted in Figure 6d.

## 5 Possible Encryption for JPEG Compression

In order to apply compression of the generated image containing the background image (e.g. visible image located in the LF parts of spectral domains) and the encrypted one (e.g. invisible image located in the HF parts of the spectral domains), we are performing the following procedure. Due to JPEG compression the original background and encrypted image are splitting on blocks size 8×8 pixels, as depicted in Fig. 7. Then for each block the DCT coefficients are determined.


**Figure 5.** The original images used in encryption method

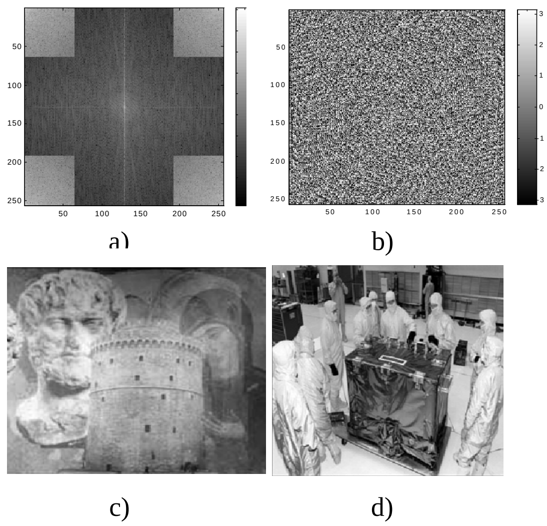



**Figure 6.** Encryption procedure in the transform domain

Inside each block the procedure described in the previous chapter is performed. The … of DCT coefficients of the background image, say the image as in Fig. 8a, is placed in the LF part of the spectral domain inside each appropriate block, preserving the original position, according to zig-zag scan [7],[8]. The ¾of DCT coefficients of the encrypted image, for instance, as in Fig. 8b, are placed in the rest of the spectral part of the appropriate block, and may be displaced by using some security key. The interior of each DCT block is shown in Fig.9.

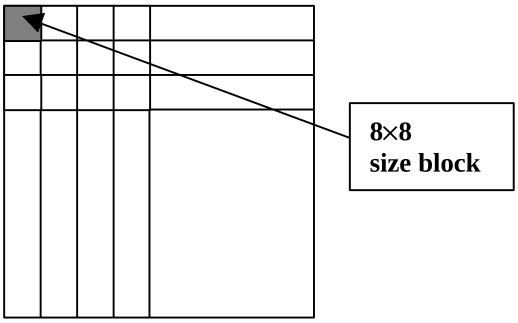
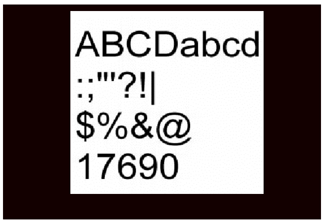



**Figure 7**. Splitting the image into 8x8 size blocks

a)




b)

**Figure 8.** The background and the encrypted images.

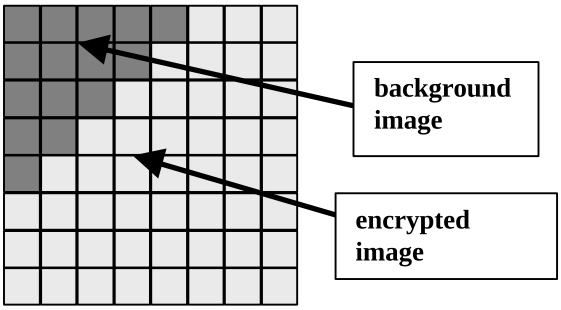
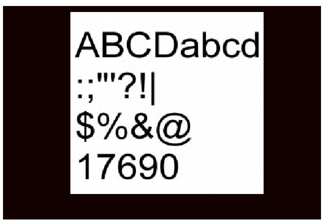



**Figure 9**. Interior of the 8x8 block in the DCT domain

By applying this procedure we are generating the complex DCT matrix consisting of the described blocks. After IDCT procedure the image as in Fig. 10a is obtained. On the receiving side, following the inverse procedure, we can reconstruct the hidden (encrypted) image, and the final result is presented in Fig. 10b.

a)




b)

**Figure 10.** (a) The background image (visible) and (b) encrypted image after the reconstruction

Note that if we decrease the number of encrypted image spectral components from ¾ to …, we can transmit two more images being are also hidden by the background image. In that way three images are encrypted, and can be reconstructed on the receiving side by their … of the spectral coefficients.

## 6 Conclusion

Here we described one possible method for the secure transfer of several images using the same frame. The algorithm exposed is presented by using the basic spectral features of digital images.

By using the fact that the main part of the signal energy is concentrated in the LF part of the spectral domain it is possible to reconstruct the image, retaining satisfactory quality, by using only the LF part of the image spectra. Regarding that, in the spectral matrix the existence of the empty part appears. In that empty part the spectral components of several images, we want to be encrypted, are placed. The amount of the preserved spectral component is significant in determining the number of encrypted images and appropriate reconstruction quality.

The algorithm exposed is an initial investigation and does not require powerful performing equipment, and it can be easily performed in a common software environment.


*References:*

[1] I. Pitas, T. Kaskalis, Applying signatures on digital images , in *Proc. IEEE Nonlinear Signal and Image Processing*, June 1995, pp. 460-463.

[2] I. Pitas, A method for watermarking casting on digital images ,*IEEE Trans. Circuits and Systems for Video Technology*., Vol. 8, No. 6, October 1998.

[3] J. Lim, *Two-Dimensional Signal and Image Processing*, Prentice-Hall, NJ, 1990

[4] M. Hayes, The reconstruction of a multidimensional sequence from the phase or magnitude of its Fourier transform ,*IEEE Trans. Acoust., Speech, and Sig. Proc.*, Vol. ASSP-30, April 1982, pp.140-154

[5] Z. Grytskiv, S. Voloshynovskiy, Y. Rytsar, Cryptography and steganography of video information in modern communications , in *Proc. Conf. TELSIKS-97*, Ni (Yugoslavia), Oct. 1997.

[6] I. RakoŁeviæ, P. Kostiæ, D. Dujkoviæ, B. Reljin, Multiple image transfer using the same spectral matrix , in *Proc. Conf. TELFOR-97*, Belgrade, Nov. 1997.

[7] R. Jain, R. Kasturi, B. Schunck, *Machine Vision*, McGraw-Hill, New York, 1995
[8] B. Jähne, *Digital Image Processing*, Springer – Verlag, Berlin-Heidelberg, 1995